UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/517,608	03/02/2000	Simon Robert Walmsley	AUTH10US	4148

7590 06/09/2005

Kia Silverbrook
Silverbrook Research Pty Ltd
393 Darling Street
Balmain, 2041
AUSTRALIA

EXAMINER	
NGUYEN, NGA B	

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 06/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/517,608	Applicant(s) WALMSLEY, SIMON ROBERT
	Examiner Nga B. Nguyen	Art Unit 3628

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8,9,11-19,21,22 and 24-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8,9,11-19,21,22 and 24-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is the answer to the Amendment filed on January 24, 2005, which paper has been placed of record in the file.

2. Claims 7, 10, 20, and 23 have been canceled.

Claims 1-6, 8, 9, 11-19, 21, 22, and 24-27 are pending in this application.

Response to Arguments/Amendment

3. Applicant's arguments with respect to claims 1-6, 8, 9, 11-19, 21, 22, and 24-27 have been considered but are moot in view of new ground of rejections.

4. Applicant's amendment necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-6, 8, 9, 11-19, 21, 22, and 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shigenaga, U.S. Patent No. 4,710,613, in view of Lee, U.S. Patent No. 5,923,759.

Regarding to claim 1, Shigenaga discloses a consumable authentication protocol for validating the authenticity of an untrusted authentication chip (column 6, lines 1-53, IC card 2 is equivalent to the untrusted authentication chip), the protocol includes the steps of:

generating an original random number in a trusted authentication chip (column 7, lines 45-48; a random number is generated from random number data generator 120 of card terminal 1, card terminal 1 is equivalent to a trusted authentication chip);

applying, in the trusted authentication chip, an asymmetric encrypt function to the original random number using a first key from the trusted authentication chip to produce a first encrypted outcome (column 7, lines 59-60, the RSA encrypter 121 in the card terminal 1 encrypts the random number using public key code, the card terminal 1 is equivalent to the trusted authentication chip, RSA encryption is asymmetric encryption function);

passing the first encrypted outcome to the untrusted authentication chip (column 7, lines 60-67, the encryption data, i.e. the encrypted random number is sent to IC card 2 from card terminal 1);

decrypting, in the untrusted authentication chip, the first encrypted outcome with an asymmetric decrypt function using a second secret key from the untrusted authentication chip to produce a second decrypted outcome (column 7, line 65-column 8, line 12; decrypting in the IC card 2 the encrypted random number by the RSA decrypter 263 using the private key code from the IC card 2);

comparing the decrypted random number and the decrypted data message with the original random number and the received original data message, without knowledge of the second secret key; and in the event of a match, considering the untrusted chip and the data message to be valid; otherwise considering the untrusted chip and the data message to be invalid (column 8, lines 28-42, 63-66, the decrypted random number is compared with the original random number by the comparison unit 15, without knowledge of the private key code stored in the IC card 2).

Shigenaga does not disclose applying, in the untrusted authentication chip, an asymmetric encrypt function to the second decrypted outcome together with an original data message read from the untrusted authentication chip using the second secret key to produce a third encrypted outcome; passing the third outcome together with the original data message to the trusted authentication chip; decrypting, in the trusted authentication chip, the third encrypted outcome with an asymmetric decrypt function using the first key to produce a decrypted random number and a decrypted data

message. In Shigenaga, the IC card 2 sends the decryption data to the card terminal 1, the IC card 2 does not encrypt the decryption data using the private key before sending to the card terminal 1, thus card terminal 1 does not decrypt the encrypted data using the public key. Thus, the IC card 2 only performs decrypt function using the private key, the terminal card 1 only performs encrypt function using the public key. However, Lee discloses the IC card performs both encrypt and decrypt function using an internal key stored in the card and the terminal card performs both encrypt and decrypt function using an identifying key stored in memory (column 6, lines 37-67). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify Shigenaga's to adopt the teaching of Lee for the purpose of improving the security, because the IC card 2 can apply the encrypt function using a secret key to encrypt the decryption data before sending to the card terminal 1, the card terminal 1 can apply the decrypt function using the public key to decrypt the encrypted data, thus the communication from the IC card 2 to the card terminal 1 is more secure with the encrypted data.

Moreover, Shigenaga and Lee do not disclose the untrusted authentication chip is contained within a consumable device and the trusted authentication chip is contained within a consuming device. However, Examiner submits that the claimed invention recites an intended use, although Shigenaga and Lee fail to discuss the intended use which is the untrusted authentication chip is contained within a consumable device and the trusted authentication chip is contained within a consuming device, Shigenaga and Lee's authentication protocol is capable for validating the

authenticity of the untrusted authentication chip as claiming in the claimed invention. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify Shigenaga and Lee's to include the feature above for the purpose of validating the authenticity of the untrusted authentication chip in a specific product such as consumable device.

Regarding to claim 2, Shigenaga discloses for validating the authenticity of an untrusted authentication chip, as well as ensuring that the authentication chip, lasts only as long as the consumable including the further steps of writing new data to the untrusted chip, performing the steps of claim 1, and in the event the untrusted is found to be authentic and the new data is the same as the data message read from the untrusted chip, then the write is validated (column 7, lines 5-30; storing the PIN send from card terminal 1 in IC card 2, comparing the stored PIN with the original PIN).

Regarding to claim 3, Shigenaga discloses the first key is a public key (column 7, lines 50-60).

Regarding to claim 4, Shigenaga discloses encryption outside the untrusted chip is implemented in software (column 8, lines 59-62; the encryption is implemented based on the RSA algorithm).

Regarding to claim 5, Shigenaga discloses the random number generation, encryption, passing, and final decrypting and comparing steps take place in an external system (column 5, line 20-column 6, lines 55, the random number generator, encryptor and comparison means are in the card terminal 1, the IC card 2 is the consumable).

Regarding to claims 6 and 9, Shigenaga does not teach the external system is in a printer or other device in which consumables such as ink cartridges are mounted, and the second authentication chip and system are in a printer or other device in which consumables are mounted. However, a printer or other devices in which consumables such as ink cartridges are mounted such as copy machine, camera, etc... are well known devices. Therefore, it would have been obvious to apply Shigenaga's cryptography method modified by Lee above for those devices for the purpose of prevent the unauthorized person to use such devices.

Regarding to claim 8, Shigenaga discloses the encryption outside the untrusted chip is implemented in a second authentication chip, and an external system intermediated between the two chips (column 8, lines 13-42).

Regarding to claim 11, Shigenaga discloses the secret key is held only by the untrusted chip (column 8, lines 1-12, private key code stored in the IC card 2).

Regarding to claim 12, Shigenaga does not teach the trusted authentication chip contains a random function to produce random numbers from a seed, and the function advances after every successful authentication so that the next random number will be produced from a different seed, for a group of authentication chips, the initial seed for each chip is different from that of the others in the group so that the first random number produced by each chip in the group will be different. However, it is well known to generate the next random number using a different seed in order to improve the level of security, and to use a different initial seed for each chip in the group of chip. Therefore, it would have been obvious to modify Shigenaga's modified by Lee above to include this

feature for the purpose of providing high security level because each next random number is generated from a different seed and each chip has a different initial seed, thus the unauthorized person cannot easily to predict the random number.

Regarding to claim 13, Shigenaga discloses the data message is a memory vector of the authentication chip, a part is different for each chip, and parts of it are constant (read only) for each consumable, or decrement only so that it can be completely downcounted only once for each consumable (column 5, lines 20-67; data message is memory of the card terminal 1).

Regarding to claim 14, Shigenaga discloses a consumable authentication system includes:

a random number generator to generate an original random number in a trusted authentication chip (figure 2 and column 5, lines 20-31, random number generator 120 included in the card terminal 1);

an asymmetric encryptor to encrypt the generated original random number with an asymmetric encryption function to produce a first encrypted outcome and using a first key for the encryptor (figure 2 and column 5, lines 38-67; the RSA encrypter 121 in the card terminal 1);

an untrusted authentication chip, the untrusted authentication chip including a read function which operates to decrypt the fist encrypted outcome using a second secret key and produce a second decrypted outcome (column 6, lines 1-55; column 7, line 65-column 8, line 12; the IC card receives the encrypted random number from the

card terminal 1, the IC card 2 includes the RSA decrypter 263 to decrypts the encrypted random number using a private key code to produce a decrypted random number); and

a test function, the test function compares the decrypted random number and decrypted data message with the generate original random number and the received original data message, without knowledge of the second secret key; whereby, in the event of match the test function returns a valued indicating validity; otherwise it returns a value indicating invalidity (figure 2, column 2, lines 62-67 and column 8, lines 28-32, 63-66, the comparison unit 15 compares the decrypted random number with the original random number, without knowledge of the private key code stored in the IC card 2).

Shigenaga does not disclose the untrusted authentication chip then applies the symmetric encrypt function to the second decrypted outcome together with an original data message read using the second secret key to produce a third encrypted outcome, also retuning the third encrypt outcome together with the original data message; the test function operating to decrypt the third encrypt outcome using the first key to produce a decrypted random number and a decrypted data message. See claim 1 above for the same motivation.

Moreover, Shigenaga and Lee do not disclose the untrusted authentication chip is contained within a consumable device and the trusted authentication chip is contained within a consuming device. However, Examiner submits that the claimed invention recites an intended use, although Shigenaga and Lee fail to discuss the intended use which is the untrusted authentication chip is contained within a consumable device and the trusted authentication chip is contained within a consuming device, Shigenaga and

Lee's authentication protocol is capable for validating the authenticity of the untrusted authentication chip as claiming in the claimed invention. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify Shigenaga and Lee's to include the feature above for the purpose of validating the authenticity of the untrusted authentication chip in a specific product such as consumable device.

Claims 15-19, 21, 22, 24-27 contain similar limitations found in claims 2-6, 8, 9, 11-13, discussed above, therefore are rejected by the same rationale.

Conclusion

7. Claims 1-6, 8, 9, 11-19, 21, 22, and 24-27 are rejected.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is (571) 272-6796. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Sough can be reached on (571) 272-6799.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-3600.

9. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

C/o Technology Center 3600

Washington, DC 20231

Or faxed to:

(703) 872-9306 (for formal communication intended for entry),

or

(571) 273-0325 (for informal or draft communication, please label "PROPOSED" or "DRAFT").

Hand-delivered responses should be brought to Knox building, 401 Dulany Street, Alexandria, VA, First Floor (Receptionist).

Nga B. Nguyen
Nga Nguyen
April 15, 2005